Attorney Docket No. 1032326-000301

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of

Marc Joye et al.

Application No.: 10/534,873

Filed: November 22, 2005

For: INTEGER DIVISION METHOD SECURE AGAINST COVERT CHANNEL ATTACKS

MAIL STOP
APPEAL BRIEF - PATENTS

Group Art Unit: 2431

Examiner: BRYAN F WRIGHT

Appeal No.: _____

APPEAL BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This appeal is from the decision of the Primary Examiner dated January 25, 2010, finally rejecting claims 1-13, which are reproduced as the Claims Appendix of this brief.

☒ Charge ☐ $ 270 ☒ $ 540 to Credit Card. Form PTO-2038 is attached.

The Commissioner is hereby authorized to charge any appropriate fees under 37 C.F.R. §§ 1.17 and 41.20 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 02-4800.

08/17/2010 AWONDAF1 00000111 10534873
01 FC:1402 540.00 OP

08/17/2010 AWONDAF1 00000113 10534873
01 FC:1402 540.00 OP

Table of Contents

I. Real Party in Interest

GEMALTO SA, which is the successor in interest to GEMPLUS, the original assignee of the application, is the real party in interest.

II. Related Appeals and Interferences

The Appellants' legal representative, or assignee, does not know of any other appeals, interferences or judiciary proceedings which will affect or be directly affected by or have bearing on the Board's decision in the pending appeal.

III. Status of Claims

The application contains claims 1-13. To simply issues for the appeal, claims 3, 6, 10 and 11 are being cancelled in a supplemental Amendment filed concurrently with the Appeal Brief. Accordingly, claims 1, 2, 4, 5, 7-9, 12 and 13 are currently pending. Claims 1, 2, 4, 5, 7-9, 12 and 13 stand finally rejected, and are being appealed.

IV. Status of Amendments

A supplemental Amendment is being filed concurrently herewith, canceling claims 3, 6, 10 and 11. For purposes of this appeal, it is assumed that this Amendment will be entered, since it complies with the requirements of 37 C.F.R. § 41.33(b)(1).

No other amendments were filed subsequent to the final Office Action dated January 25, 2010.

V. Summary of Claimed Subject Matter

The claimed subject matter is directed to a cryptographic method that employs integer division.

Pursuant to 37 C.F.R. §41.37(1)(c)(v), the subject matter of independent claim 1 is cross-referenced to the specification in the following table. The following table is not to be construed as a representation that the portions of the disclosure identified below constitute the sole basis for support for the claimed subject matter.

Claim	Disclosure
1. A cryptographic method during which an integer division of the type q = a div b and r = a mod b is performed in a processor of an electronic device, where q is a quotient, a is a number containing m bits, b is a number containing n bits, with n less than or equal to m and b_{n-1} is non-zero, b_{n-1} being the most significant bit of b, comprising the following steps:	Page 9, the second full paragraph
(i) performing a partial division of a word A, comprising n bits of the number a, by the number b to obtain a bit of the quotient q, wherein at least one of the numbers a and b comprises secret data;	Page 9, the third full paragraph
(ii) repeating step (i) for m-n+1 iterations with the same number and type of operations being performed at each iteration, regardless of the value of the quotient bit obtained, to obtain the quotient q; and	Page 9, the third full paragraph - page 10, the first full paragraph
(iii) generating encrypted or decrypted data in accordance with said quotient.	Page 10, line 2

VI. Grounds of Rejection to be Reviewed on Appeal

Claims 1, 2, 4, 5, 7-9, 12 and 13 stand finally rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Menezes ("Handbook of Applied

Cryptography") in view of Drexler et al. (U.S. Patent Application Publication No. 2003/0061498).

VII. Argument

Claims 1, 2, 4, 5, 7-9, 12 and 13 stand finally rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over the Menezes reference, in view of the Drexler patent application. The rejection should be withdrawn at least because the Menezes reference and the Drexler patent application, whether considered individually or in combination, do not disclose each feature in Appellants' claims.

A. Appellants' Exemplary Embodiments

Appellants' exemplary embodiments relate to an integer division method that is secured against covert channel type attacks. It is well known that a covert channel attack includes an attack based on a physical quality measurable from outside a device such as a smartcard, and whose analysis makes it possible to discover data contained and manipulated in processing operations performed in the device. See Appellants' specification: the paragraph bridging pages 1 and 2. Physical quantities that are exploited during attacks include execution time, the current consumption, the electromagnetic field radiated by the part of component used for executing the calculation, etc. See the specification: page 2, the first full paragraph. These attacks are based on the fact that, during the execution of a method, the manipulation of a bit leaves a particular imprint on the physical quantity in question, according to the value of this bit and/or according to the instruction. For example, a method including iterations is sensitive to covert channel attacks if at each iteration of the method, the

number of operations performed during the iteration varies according to the result bit obtained during the iteration.

Method 1, as described in pages 4-7 of the specification, is a known method of integer division that is sensitive to covert channel attacks. According to Method 1, at each iteration, based on the value of the quotient bit which will be obtained during the current iteration, it is determined whether an ADD step is performed or not. The number of operations performed during an iteration, therefore, varies according to the result bit obtained during the iteration. See the specification: page 6, the last full paragraph. The current consumption during each iteration and/or the duration of each iteration varies according to the number of operations performed. *Id.* By measuring and studying for example the trace left by the component when the method is executed, it is possible to determine bit by bit the value of the result bits. *Id.*

According to Appellants' exemplary embodiments, an integer division is performed for a cryptographic method with the same number and type of operations at each iteration, regardless the value of the bit obtained, so that the method is secured against covert channel attacks. For example, according to Appellants' exemplary embodiments described in pages 9 and 10 of the specification, an integer division can be performed with the following steps:

For j = 1 to (m-n+1), do:

$a \leftarrow SHL_{m+1}(a, 1)$; $\sigma \leftarrow$ carry

$A \leftarrow (\sigma')SUB_n(A, b) + (\neg\sigma')ADD_n(A, b)$

$\sigma \leftarrow (\sigma' \text{ AND } \sigma') / (\sigma' \text{ AND carry}) / (\sigma' \text{ AND carry})$

lsb(a) σ

$\sigma' <- \sigma$

End For

In the above example, during each iteration of the "For Loop," the number of operations performed is the same. It is not dependent upon the results that are produced. As such, the integer division method according to Appellants' exemplary embodiments is not sensitive to covert channel attacks.

B. Claim 1

Claim 1 recites a cryptographic method during which an integer division of the type q = a div b and r = a mod b is performed in a processor of an electronic device, the method comprising, *inter alia*,

> (i) performing a partial division of a word A, comprising n bits of the number a, by the number b to obtain a bit of the quotient q, wherein at least one of the numbers a and b comprises secret data;
>
> (ii) repeating step (i) for m-n+1 iterations with the same number and type of operations being performed at each iteration, regardless of the value of the quotient bit obtained, to obtain the quotient q. (emphasis added)

The Examiner acknowledges that the Menezes reference does not disclose "(ii) repeating step (i) for m-n+1 iterations with the same number and type of operations being performed at each iteration, regardless of the value of the quotient bit obtained, to obtain the quotient q," as recited in claim 1. However, the Examiner relies upon section 14.20 of the Menezes reference, and asserts that the reference discloses instructions implemented as a Computer For Loop Condition Statement for iterative calculation of the encryption process. The Examiner further asserts that the claimed method is a minor change of the "For Loop" instruction to be iterated through the encryption process, as disclosed in the Menezes reference. See the Office

Action dated January 25, 2010, page 4, the first and second full paragraphs. Appellants respectfully disagree.

The Menezes reference discloses division of number x by number y, wherein $x=qy+r$, $x=(x_n...x_1x_0)_b$, and $y=(y_t...y_1y_0)_b$. Referring to section 14.2.5, Algorithm 14.20 of the Menezes reference, a Multiple-precision division method includes the following steps:

3. For i from n down to $(t+1)$ do the following:
   3.1 If $x_i = y_t$ then set $q_{i-t-1} \leftarrow b-1$; otherwise set $q_{i-t-1} \leftarrow \lfloor (x_i b + x_{i-1})/y_t \rfloor$.
   3.2 While $(q_{i-t-1}(y_t b + y_{t-1}) > x_i b^2 + x_{i-1} b + x_{i-2})$ do: $q_{i-t-1} \leftarrow q_{i-t-1} - 1$.
   3.3 $x \leftarrow x - q_{i-t-1} y b^{i-t-1}$.
   3.4 If $x < 0$ then set $x \leftarrow x + y b^{i-t-1}$ and $q_{i-t-1} \leftarrow q_{i-t-1} - 1$.

According to the method in the Menezes reference, the number or type of operations performed at one iteration might be different from another iteration. In step 3.1 of the Algorithm, it can be seen that the value for the expression "q_{i-t-1}" varies in dependence upon whether $x_i = y_t$. In step 3.2 of the Algorithm, the operation in the "While Loop" repeatedly executes until the expression in the While condition no longer holds true. Since, for each iteration, the values in the expression of the While condition may be different, the number of operations performed is not guaranteed to be the same for each iteration.

In addition, according to step 3.4 in the Algorithm, the steps set $x \leftarrow x + y b^{i-t-1}$ and $q_{i-t-1} \leftarrow q_{i-t-1} - 1$ are performed for an iteration, only when the current value of x in that iteration is less than zero. Given that x is defined as a positive integer (see "INPUT" for the Algorithm), the current value of x for some iterations can be greater than or equal to zero. Consequently, the number and type of operations performed are not necessarily the same for each iteration of the Algorithm in the Menezes reference.

In contrast, according to Appellants' exemplary embodiments, the same number and type of operations are performed at each iteration. For example, according to Appellants' exemplary embodiments described in pages 9 and 10 of the specification, the following steps are performed in each iteration, regardless of the values obtained during each iteration:

$a \leftarrow SHL_{m+1}(a, 1)$; $\sigma \leftarrow$ carry

$A \leftarrow (\sigma')SUB_n(A, b) + (\neg\sigma')ADD_n(A, b)$

$\sigma \leftarrow (\sigma' \text{ AND } \sigma') / (\sigma' \text{ AND carry}) / (\sigma' \text{ AND carry})$

lsb(a) σ

$\sigma' \leftarrow \sigma$

Unlike the Algorithm of Menezes, this sequence of steps does not contain conditional "If" or "Where" statements that can affect the number of operations performed. As such, the method in the Menezes reference is sensitive to covert channel attacks because at each iteration of the method, the number of operations performed during the iteration varies according to the result bit obtained during the iteration. In contrast, claim 1 recites repeating step (i) for m-n+1 iterations with the same number and type of operations being performed at each iteration, regardless of the value of the quotient bit obtained, to obtain the quotient q.

Contrary to the assertion by the Examiner, the claimed method is not a minor change of the "For Loop" instruction to be iterated through the encryption process, disclosed in the Menezes reference. There are meaningful differences between the claimed method and the method disclosed in the Menezes references. The Menezes reference does not disclose an integer division method that is not sensitive to covert channel attacks because according to the reference, the number or the

type of operations performed for each iteration is conditioned upon the result that is obtained. Whereas, the claimed method is not sensitive to covert channel attacks because the same number and type of operations are performed at each iteration.

In the Advisory Action dated May 27, 2010, the Examiner asserts that "the 'For' loop of Menezes as illustrated could possibly produce the same result as applicant's 'For' loop with equal or less iterations." The Examiner further asserts that discounting Menezes based on the number of division iteration operations performed and the subjective opinion describing the susceptibility of the Menezes reference to attacks are not sufficient to overcome the rejection.

Appellants submit that the Examiner's understanding of Appellants' invention is incorrect. Appellants do not contend that the 'For' loop of Menezes produces the result as applicant's 'For' loop with more or less iterations. The actual number of iterations is not the issue. Rather, the pertinent question is whether the same number and type of operations are being performed at each iteration, regardless of the value of the quotient bit obtained, as recited in claim 1.

In addition, the Appellants' argument that the method disclosed in the Menezes reference is sensitive to covert channel type attacks is not a subjective opinion. Rather, the Appellants' argument is based on the fact that the number or type of operations performed at one iteration in the Menezes reference might be different from another iteration.

Appellants submit that the Examiner has applied the Menezes reference to claim 1 by simplifying the claimed method as disclosing a "For" loop statement, and has not appreciated the meaning of the recitation "same number and type of operations being performed at each iteration" in Appellants' claim 1.

Drexler, relied upon for allegedly disclosing that at least one of the numbers a and b comprises secret data, and generating encrypted and decrypted data in accordance with said quotient, does not remedy the above-noted deficiencies of the Menezes reference.

In view of the foregoing, claim 1 is patentable. Claims 2, 4, 5, 7-9, 12 and 13 are patentable at least because of their dependency from claim 1.

C. Claim 2

Claim 2 recites at each iteration, an addition of the number b to the word A and a subtraction of the number b from the word A are performed. In claim 2, for the integer division of the type q = a div b and r = a mod b, wherein a is a number containing m bits, and b is a number containing n bits, the word A comprises n bits of the number a.

According to Appellants' exemplary embodiments described in pages 9 and 10 of the specification, the following step is performed in each iteration:

$A \leftarrow (\sigma')SUB_n(A, b) + (\neg\sigma')ADD_n(A, b)$

The Examiner asserts that the above-recited features of claim 2 are disclosed by step 3.1 in Algorithm 14.20 of the Menezes reference. Appellants respectfully disagree.

Step 3.1 in Algorithm 14.20 of the Menezes reference provides the following:

3.1 If $x_i = y_t$ then set $q_{i-t-1} \leftarrow b - 1$; otherwise set $q_{i-t-1} \leftarrow \lfloor (x_i b + x_{i-1})/y_t) \rfloor$.

It is submitted that step 3.1 of the Menezes Algorithm does not disclose an operation in which the same value (b) is both added to and subtracted from a given word (A).

In view of the foregoing, claim 2 is patentable for those additional reasons.

D. Claim 4

Claim 4 recites that at each iteration, either the number b or a number $\bar{b}$ complementary to the number b is added to the word A.

The Examiner asserts that the above-recited features of claim 4 are disclosed by Algorithm 14.20 of the Menezes reference. Appellants respectfully disagree.

The Examiner merely makes a conclusory statement that the reference discloses claimed subject matter, with only a reference to Algorithm 14.20. However, the Examiner does not identify what is considered to be the claimed number and its complement. Accordingly, Examiners fails to meet his burden of establishing a prima facie case of obviousness for claim 4.

In view of the foregoing, claim 4 is patentable for those additional reasons.

E. Claim 5

Claim 5 depends from claim 4 and recites, at each iteration, updating a first variable (σ') indicating whether, during the following iteration, the number b or the number $\bar{b}$ is to be added with the word A according to the quotient bit produced.

The Examiner asserts that the above-recited features of claim 5 are disclosed by Algorithm 14.20 of the Menezes reference. Appellants respectfully disagree.

In the Office Action, the Examiner refers to "x" as the claimed variable (σ'). However, in the Menezes reference, "x" is the input to the algorithm, not a process variable that corresponds to the first variable (σ'), as described in claim 5.

In addition, in the Menezes reference, there is no disclosure the value of "x" indicats whether, during the following iteration, the number b or the number $\bar{b}$ is to be added with the word A.

According, the Menezes reference fails to disclose a method including "at each iteration, updating a first variable (σ') indicating whether, during the following iteration, the number b or the number $\bar{b}$ is to be added with the word A according to the quotient bit produced," as recited in claim 5.

In view of the foregoing, claim 5 is patentable for those additional reasons.

F. Claim 7

Claim 7 recites at each iteration, performing an operation of complement to 2^n of an updated data item (b or $\bar{b}$) or of a notional data item (c or $\bar{c}$), and adding the updated data item with the word A.

The Examiner asserts that the above-recited features of claim 7 are disclosed by Algorithm 14.20 of the Menezes reference. Appellants respectfully disagree.

As mentioned above, the Menezes reference fails to disclose the claimed number A or $\bar{b}$.

At least for those reasons, the Menezes reference fails to disclose the features in claim 7. Therefore, claim 7 is patentable for those additional reasons.

G. Claim 8

Claim 8 depends from claim 7 and recites, at each iteration, updating a second variable (δ), indicating whether, during the following iteration, the operation of

complement to 2^n is to be performed on the updated data item or on the notional data item.

The Examiner asserts that the above-recited features of claim 8 are disclosed by section 14.20 of the Menezes reference. Appellants respectfully disagree.

As mentioned above, the Menezes reference does not disclose updating a variable in a current iteration, indicating values of a variable to be used for operations in the next iteration. According, the Menezes reference fails to disclose a method including "at each iteration, updating a second variable (δ), indicating whether, during the following iteration, the operation of complement to 2^n is to be performed on the updated data item or on the notional data item," as recited in claim 8.

In view of the foregoing, claim 8 is patentable for those additional reasons.

H. Claim 9

Claim 9 recites at each iteration, updating a third variable (β) indicating whether the updated data item is equal to the data item b or to its complement to 2^n.

The Examiner asserts that the above-recited features of claim 8 are disclosed by section 14.20 of the Menezes reference. Appellants respectfully disagree.

The Menezes reference fails to disclose a number that is complement of number y to 2^n. At least for those reasons, the Menezes reference fails to disclose the features in claim 9. In view of the foregoing, claim 9 is patentable for those additional reasons.

I. Conclusion

Since the Menezes reference, even if considered in combination with the Drexler patent application, does not disclose each feature in claim 1, or its various dependent claims, claims 1, 2, 4, 5, 7-9, 12 and 13 are patentable over the references.

VIII. Claims Appendix

See attached Claims Appendix for a copy of the claims involved in the appeal.

IX. Evidence Appendix

None

X. Related Proceedings Appendix

None

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date August 16, 2010

By: Weiwei Y. Stiltner
Weiwei Y. Stiltner
Registration No. 62979

Customer No. 21839
703 836 6620

VIII. CLAIMS APPENDIX

The Appealed Claims

1. A cryptographic method during which an integer division of the type q = a div b and r = a mod b is performed in a processor of an electronic device, where q is a quotient, a is a number containing m bits, b is a number containing n bits, with n less than or equal to m and b_{n-1} is non-zero, b_{n-1} being the most significant bit of b, comprising the following steps:

(i) performing a partial division of a word A, comprising n bits of the number a, by the number b to obtain a bit of the quotient q, wherein at least one of the numbers a and b comprises secret data;

(ii) repeating step (i) for m-n+1 iterations with the same number and type of operations being performed at each iteration, regardless of the value of the quotient bit obtained, to obtain the quotient q; and

(iii) generating encrypted or decrypted data in accordance with said quotient.

2. A method according to Claim 1, wherein, at each iteration, an addition of the number b to the word A and a subtraction of the number b from the word A are performed.

4. A method according to Claim 1 wherein, at each iteration, either the number b or a number $\bar{b}$ complementary to the number b is added to the word A.

5. A method according to Claim 4, further including the step, at each iteration, of updating a first variable (σ') indicating whether, during the following

iteration, the number b or the number $\bar{b}$ is to be added with the word A according to the quotient bit produced.

7. A method according to Claim 1, further including the steps, at each iteration, of performing an operation of complement to 2^n of an updated data item (b or $\bar{b}$) or of a notional data item (c or $\bar{c}$), and adding the updated data item with the word A.

8. A method according to Claim 7, further including the step, at each iteration, of updating a second variable (δ), indicating whether, during the following iteration, the operation of complement to 2^n is to be performed on the updated data item or on the notional data item.

9. A method according to claim 7, further including the step, at each iteration, of updating a third variable (β) indicating whether the updated data item is equal to the data item b or to its complement to 2^n.

12. An electronic component comprising calculation means programmed to implement a method according to claim 1, said calculation means comprising a central unit associated with a memory comprising several registers for storing the data a and b.

13. A chip card comprising an electronic component according to Claim 12.

IX. EVIDENCE APPENDIX

None

X. RELATED PROCEEDINGS APPENDIX

None